A SECURE VOICE SYSTEM WITH BANDWIDTH REDUCTION

Fidel L. Baca

THESIS

A SECURE VOICE SYSTEM WITH BANDWIDTH REDUCTION

by

Fidel L. Baca

Thesis Advisor: O. M. Baycura

March 1976

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) A Secure Voice System With Bandwidth Reduction		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis; March 1976 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Fidel L. Baca		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		12. REPORT DATE March 1976 13. NUMBER OF PAGES
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) Naval Postgraduate School Monterey, California 93940		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Bandwidth, secure voice system

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The need for secure voice communication systems is increasing both in the civil and military arenas. Coupled with this is the need for conserving bandwidth, increasing performance, and reducing costs. Currently used secure voice methods are relatively antiquated and do not provide desired performance and bandwidth conservation without incurring increasing costs. A new system, proposed herein offers bandwidth reduction, increased performance, and decreasing costs while using modern digital techniques as opposed to analog techniques. The proposed system, known as VOCOM, operates in existing

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601 |
(Page 1)

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

voice bandwidths using existing equipment, and offers a higher level of privacy and security while at the same time simplifying software handling. Additionally, the proposed system offers the user real-time operation to enhance critical decision-making.

A SECURE VOICE SYSTEM WITH BANDWIDTH REDUCTION

by

Fidel L. Baca
Lieutenant Commander, United States Navy
B.A., Naval Postgraduate School, 1970

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL

March 1976

ABSTRACT

The need for secure voice communication systems is increasing both in the civil and military arenas. Coupled with this is the need for conserving bandwidth, increasing performance, and reducing costs. Currently used secure voice methods are relatively antiquated and do not provide desired performance and bandwidth conservation without incurring increasing costs. A new system, proposed herein offers bandwidth reduction, increased performance, and decreasing costs while using modern digital techniques as opposed to analog techniques. The proposed system, known as VOCOM, operates in existing voice bandwidths using existing equipment, and offers a higher level of privacy and security while at the same time simplifying software handling. Additionally, the proposed system offers the user real-time operation to enhance critical decision-making.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

The need for security in voice communications systems is steadily increasing. Sensitive information is constantly being passed between people which, if intercepted by unintended or undesireable elements, could significantly affect the original purpose of the communication. As a consequence, the communicating parties stand to lose money, position, status or crucial elements of their own livelihood including national or personal security. Some protection methods are relatively antiquated and ineffective, Compared to the current electronic "state of the art" for intercepting uncovered transmissions as well as covered transmissions.

Voice security requirements reach into wide areas of business, civil and military communications. The need for voice security is obvious in credit, stockmarket, and banking operations where information transferred by voice on uncovered lines demands confidentiality. These systems are vulnerable to attack by eavesdroppers and intelligence gatherers seeking to sabotage or threaten communications. Law enforcement communication systems clearly need protection of voice communications. Although many of the police systems employ coding schemes, determined interceptors can, by patient association, break the spoken codes.

In the military voice communication applications, elaborate daily-changing coding schemes have been developed as a sophisticated method of ensuring communications security. However, determined or hostile agents need only

monitor and link several communications of the same subject matter to discern a pattern of the transmitted content. Elaborate and complex encryption schemes employed by the military necessitate computers and space-consuming software such as publications and decoding tools. Because of its large volume of usage, cost, size, and physical space requirements are usually justified by economies of scale.

There are smaller, local applications of voice security that do not require elaborate equipment, expense, or physical space requirements of larger-scale operations. The same protection afforded the larger systems, of course, would be desirable in the smaller systems but the hardware and software complexity is not justified. Congressional criticism of insecure voice equipment during the Viet Nam conflict documented a need for voice coding systems applicable to local, smaller needs. [23]

II. VOICE CODING SYSTEMS

Voice coding systems are of two general types: analog and digital. Digital systems convert voice signals directly into a number or digit stream, transmitting these bits in place of a voice signal. Existing digital systems require more than the nominal 3000 hertz bandwidth available in most telephone applications. A digital system is therefore referred to as a wideband system. Wideband is defined as being several times the unencoded base band signal width compared to a narrow band of approximately the same bandwidth [16]. The wide band virtually eliminates retrofit compatibility without extensive rework of existing communications systems. [21] Digital characteristics are well suited to systems employing pseudo-random encoding data streams. [8] Digital systems typically have analog-to-digital and digital-to-analog converters with coding and decoding of a digital data stream.

A. ANALOG SYSTEMS

Analog systems are used in voice security systems more extensively than digital systems. They are characterized by balanced mixers, oscillators and filters. The various types are discussed below. [8]

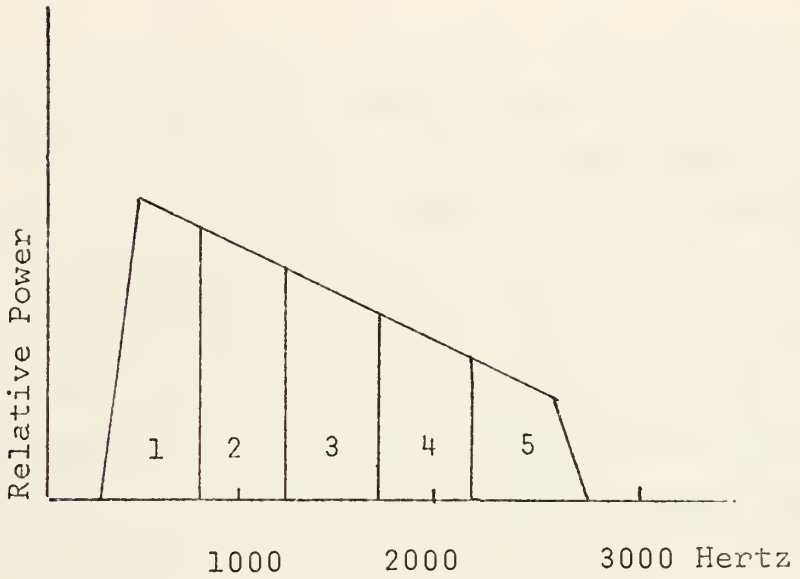
1. Inversion

Inversion is the name for a scrambling process that provides security by systematic modification of a voice signal before transmission. In its simplest form it interchanges low voice frequencies and high voice frequencies. It operates by changing each frequency component present in a voice signal to a new frequency, where the new frequency is the difference between the original frequency and the reference or inversion frequency. For example, at a reference frequency of 3000 hertz, a voice component at 750 hertz would be converted to a component at 3000-750 hertz or, 2250 hertz. A scrambled signal must be unscrambled at the receiving end using a second inverter of the same reference frequency. When the scrambled 2250 hertz frequency is subtracted from the reference frequency, 750 hertz, the original frequency voice component is restored. The ease of unscrambling inverted speech makes this system vulnerable to unsecure transmission. An eavesdropper need only use an inverter with an adjustable reference frequency oscillator, tuning the oscillator until the speech is intelligible. Moreover, with concentrated attention, inverted speech can be learned directly in about four hours. Figure 1 depicts inversion. [8]

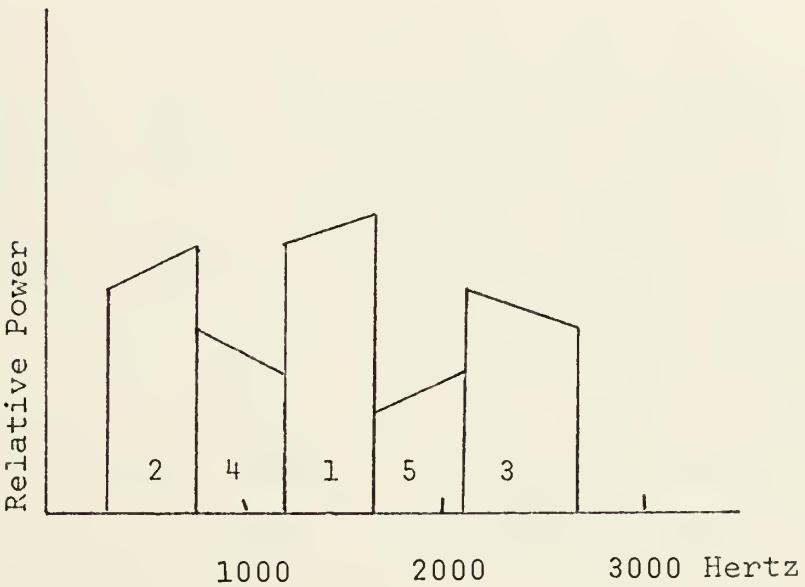
Figure 1 - INVERSION

2. Band-Splitting

A more secure method of scrambling either divides the 300-3000 hertz voice band into several subbands, or it inverts them, or both. This is known as band-splitting. Unscrambling is achieved by interchanging the signals in the subbands and reinverting them as required. Its advantage over the simple inversion technique is that many different code settings are possible according to how the different subbands are rearranged in the scambling process. Unlike the inversion technique, one cannot learn to directly understand the scrambled output of a band-splitter. However, by repeating a message several times, many of the words can be unscrambled by the human ear. It is also possible to eavesdrop by using equipment that returns just one of the subbands to its proper place thus rendering this method susceptible to relatively simple attacks. Figure 2 depicts band-splitting. [8]



(a) Original voice signal spectrum



(b) Scrambled voice signal spectrum; (note both displacement and inversion of the bands)

Figure 2 - BAND-SPLITTING

3. Masking

Security offered by inversion and band-splitting techniques can be enhanced by adding extraneous tones or ncise in a scrambler to mask the voice. These additions must be filtered out by an unscrambler. The difficulty of filtering is aggravated by the presence of harmonic distortion in transmission systems. Such distortion will generate noise and tones at new frequencies where they cannot be removed without also removing some of the voice signals. Consequently, masking increases the security of voice communication while reducing message intelligibility by the intended listener.

4. Time Domain Systems

Another security method leaves a voice signal in its original frequency components but divides a signal into time elements, transmitting the various elements in a rearranged sequence. This is known as a time domain system while the previous systems operate in the frequency domain. The time domain of an inversion system would generate speech in reverse order of time. This is not normally done in practice because a scrambler would have to wait until a complete message was expressed before it could be transmitted in reverse. This involves delays in the communications process. A better method is to divide the message in to small distinct time segments to delay for varying brief intervals before reprcducing them. This mixes the order of the voice segments while making the output unintelligble without compatible equipment. To date, these systems have required large, expensive magnetic recorders. At present there are no time dcmain scramblers on the U.S. market.

5. Changing vs. Fixed Codes

The methods discussed thus far were assumed to use fixed codes. Using a continually changing code sequence at different times increases the difficulty of intelligible interception by an eavesdropper unless he had access to the specified code sequence being used at a particular time. In a properly designed system enough different codes can be used so as to make it impractical for an eavesdropper to find the correct one. This method is enhanced even further if the code is changed as often as each day. This system requires frequent dissemination of particular codes to the users and security precautions to ensure that the codes do not fall into unauthorized hands.

B. DIGITAL TECHNIQUES

The quality of digital transmissions is affected by the number of encoding levels in the bit stream. The larger the number of levels, the more bandwidth is required to transmit the signals. Bandwidth being a scarce commodity, an increase in bandwidth usage will result in an increase in cost. Conventional digital voice security systems are characterized by by use of larger amounts of bandwidth (wideband) than analog voice security systems (narrowband). They are consequently more expensive than analog systems. Nonetheless, digital systems have technical advantages, especially when sending vast amounts of data over long distances where storing of the data is required. Sending analog signals over long distsances requires expensive lines and high quality radio links. Long telephone lines can cause drastic attenuation in high frequencies. This effect can be overcome only by the use of costly coaxial or other

special cables. In contrast, even if transmission quality is poor, a digital system need only detect whether a "0" or a "1" was sent. It need not detect complicated and detailed waveforms of speech. Much poorer signals can be acceptably decoded and no noise or interference is present in the data sent; the output will be noise and interference free.

Another method of telephone tranmission converts sounds into a stream of bits (pulse code modulation) and eliminates need for the costly modems required in analog systems. [16] The pulse code modulation (PCM) techniques being constructed equate to one channel becoming the equivalent of 56,000 bits per second in each direction. During an experiment in Europe by Martin [16] a computer, a teletype machine, and a telephone line as the communication link took place. During one observation an analog voice line capable of transmitting 4,800 bits per second was used. In a half hour it could transmit 1800 x 4,800 or 8,640,000 bits. In fact, it had only sent 21,000 bits of data. Its efficiency was 21,000/ 8,640,000 or .0024, a poor use of an expensive facility. Voice lines use PCM techniques in which one telephone channel becomes equivalent to 56,000 bits per second in each direction. This bit stream could conceivably transmit 1,800 x 56,000 bits in a half hour in each direction. Using time sharing, the transmission efficiency could then be said to be 21,000/2 x 1,800 x 56,000 or .0001. If we could push the efficiency up to .25 we would have an improvement of 2,500 times. On an analog voice line used at 4,800 bits per second, a one hundred fold improvement would result. This can be accomplished through time sharing. [16]

Analog storage is bulky and cumbersome, requiring tapes, and discs that are susceptible to damage loss, or misplacement. The use of digital storage techniques offers the user large amounts of storage capacity, fast access time, processing in real time, and minimal human handling.

A new system proposed here reduces PCM requirements from 56,000 bits per second to a mere 200 bits per second. The increased advantage goes from an efficiency of (in the example cited) .0024 to 3000 x 7/1,800 x 200 or .0583. The bit rate reduction is over 400:1. In general, a decrease in bandwidth decreases expense. Therefore, restricting the bandwidth decreases expense. This bandwidth reduction technique can be applied to voice security systems.

III. PROPOSED VOICE CODING SYSTEM

A. REASON FOR DIGITAL

In normal speech there is a considerable redundancy of expression which means that more symbols are transmitted than are required to communicate the information. Parts of words and often whole words frequently are not required to communicate effectively. Naval messages typically are reduced to acronyms, abbreviations, and shortened words which are understandable to the communicating parties. An example of redundancy is "ueue" in "queue". The "ueue" sound always follows the "q" and therefore the "ueue" is redundant. "The" is also frequently redundant. Most redundancy results from rules and limitations placed on languages, excluding usable combinations of letters. In a language permitting any permutation of four letters to be a word, such as "ngwv", then 456,976 words, or approximately the number of words in an unabridged dictionary, would exist. The English language prohibits a combination such as "ngwv", rendering it more redundant than the hypothetical four letter language. Limitations on vocabulary add to the waste. A child's use of the word "play" may be changed by an adult to "frolic" or "amusement". It is more redundant for someone to "accomplish something" than it is for someone to "do something". According to Shannon, [24] two extremes of redundancy exist: one extreme is in use of additional whole words to add emphasis to an idea; the other extreme is in superfluous inflections and drawls of various dialects. "The basic English vocabulary is limited to 850 words and

the redundancy very high. This is reflected in the expansion that occurs where a passage is translated into basic English."

Rules, limitations, formalities, and the desire to modify language and speech create redundancy. As a result, English is about 75% redundant which is to say only 25% of English text is necessary if it were wholly nonredundant. [10]

In information theory entropy must be eliminated from a system. This is precisely what the proposed digital system does. By reducing the input data to a nonredundant level, much useless data is discarded while working parts are retained. As an example, data is transferred at the rate of 60 kilobits per second in Bell Telephone digital links with enormous redundancy since human speech conveys meanings at the rate of only a few hundred bits per minute. Speech as an audio signal is limited to a data rate of only several hundred bits per second. The proposed digital system transmits speech virtually without redundancy. Known as VOCOM, (Voice COMmunication through COMpression and COMputation) it sends a series of digits that instruct a synthesizer tc recreate speech, instead of sending the original speech waveforms. Only several hundred bits, a fraction of the real amount, need be sent. [25] Because the human ear is sensitive to amplitude and frequency changes, a VOCOM processed signal will vary from the original yet still have sufficient quality to be intelligble. [17] Potential losses from data compression include recognition of who is speaking, transmission of the emotional content, and conversational effort.

B. DESIGN OF THE VOCOM SYSTEM

The design of a voice security system must be compatible with existing radio telephone equipment. It must also provide a reasonable amount of privacy against not only the "snooper" on the RF channel but also against the loss or compromise of equipment. Finally, it must be reasonable in cost. The constraint of making the security system compatible with existing equipment restricts the communication channel to 300 to 3000 hertz.

A digital computer has been designed to receive a continuous electrical signal and transform it into data at a comparatively slow rate for input into a general purpose processor. The machine uses digital circuits throughout to compute instantaneous values of frequency and power in real time. This machine is a special purpose digital computer capable of various modes of transformation through the use of Fourier transforms. This makes it easily applicable to the analysis of speech. It also allows hardware to be time-shared among several filters capable of examining components in any band of the audible spectrum. The digital filter bank, consisting of 128 filters, is capable of providing 10 octaves of data at semitone intervals to the digital oscillator bank with 64 oscillators. Although it was designed for transmitting music, its potential is great in secure voice applications. (Contact for future reference: Mr. Alan Sutcliffe, Electronics Music Studios, 277 Putney Bridge Road, London, SW152PT England.)

C. HARDWARE

The "heart" of the system relies upon the PDP-8 minicomputer manufactured by Digital Equipment Corporation (146 Main Street, Maynard, Massachusetts, 01754). It uses a 12-bit word length intended for laboratory and process control applications with original system prices of approximately $28,500. [8] Originally not called a minicomputer, it rapidly became very popular and soon became recognized as the first mass-produced and popular minicomputer and the first computer to sell for less than $20,000 (CPU only). A memory instruction can reference any of 128 addresses on its own page, or any of 128 addresses on other pages. With indirect addressing, any location in memory can be referenced. These 128 addresses coincide with the 128 filters and 64 oscillators in the VOCOM system.

The digital hardware consist of two PDP8 computers, a disc file, and a fast paper reader/punch with an attached magnetic tape drive. The input and output system makes it suitable for real-time applications. A crystal clock in the interrupt line delivers synchronizing pulses at 400 hertz or a sub-multiple of this frequency. There are also 10 kilohertz digital-to-analog and analog-to-digital converters for visual purposes. [30]

The computers control the pitch, timing, amplitude, and waveform through three banks The computers also control the gain and respose mode of 64 narrow passband filters placed at semitone intervals over five and one half octaves. Nine other oscillators and function generators, six amplifiers, two variable response filters, and a number of other devices such as noise generators are also controlled by the

computers. Most of the connections are done manually at a patch panel but up to twenty of them may be connected through computer controlled audio switches. [9]

There must first be an analog signal from a telephone, radio or other sound source. The signal is fed through a series of specialized filters and compressors to the analysis section of the VOCOM receiver still in basic audio signal form. In the next step a digital analysis occurs where a number of parameters may be varied which determine the amount of digital data to be stored or transmitted.

These varying parameters are rate analysis, normally 20-30 times a second for speech; the number of points on the frequency spectrum to be sampled; and the precise frequencies for each of these points. Up to 64 individual frequencies (individually) can be analyzed ranging from 0-16 kilohertz. For each of these points, up to 64 levels may be detected thus allowing a large amount of data to be absorbed by the receiver. [29]

The principle of operation is simple: (1) an analog signal is transmitted, (2) it is analyzed by means of a special version of a fast Fourier transform, (3) it is rearranged so as to only resemble the original contents, and (4) it is retransmitted as a series of instructions to the VOCOM receiver which then (5) reconverts it to an understandable analog signal. This system is unique in that both the receiver and the transmitter are computers. It is not data that is transmitted as much as it is precise instructions. Because these instructions require little data to cause very large changes in the final output, a data reduction is possible. This synthesizing machine is programmable in waveform, frequency, amplitude, and time of change of frequency and amplitude.

D. SOFTWARE

Specially developed programs called VOCAB and MUSYS allow real-time transformation into computer instructions. At this point data reduction eliminates redundant speech parts and keeps the meaningful parts. For example, if a spoken word is drawn out it is not necessary to continue the sound every instant until it is complete; rather, it is only necessary for a computer instruction to say "continue this sound at this rate for a certain period". The VOCOM capability of storing, mixing, and continuing sounds increases the security of voice communications. Other reductions pick out peaks in the data, calculate variations in the frequency and amplitude and identify the sound source such as a telephone. Telephone identification offers further reduction since only the bandwidth of the source is required. Data reduction eliminates normal pauses and gaps in speech. As an example of the instructions:

"do nothing for .23 seconds."

"keep on going like you are for .11 seconds."

"Change the frequency 230 hz over .13 seconds at rate X until silence."

"It is the end of a sentence. drop the overall pitch for .10 seconds at rate 4." [30]

The digital data between the receiver and transmitter can be transmitted at a rate of less than 1000 bits per second for speech and higher if it becomes necessary. It is estimated that telephone speech can be transmitted at 200

bits per second, representing a data reduction when transmitting.

To reiterate pertinent points: a digital computer is able to program 64 oscillators, each capable of producing three periodic waveforms at any amplitude. In theory the system is capable of reproducing any sound. Amplitude and frequency change is separately defined for each oscillator. A crystal clock can communicate to and from the computer giving interrupts at appropriate programmable intervals. Three output amplifiers can be digitally controlled for overall dynamic changes. [29]

E. COST CONSIDERATIONS

This system is not only reliable but also inexpensive. Hardware prices quoted by Digital Corporation, the manufacturers of the PDP8 minicomputer [3, 13] indicate that the hardware can be purchased for approximately $40,000. the figures listed below are within ten percent accuracy.

PDP8 Computer	$7,600 (2 required)
Memory Box	$5,000
Disc File	$3,950 (2 required)
Paper Tape reader/Punch	$4,200
LA 36 Terminal	$2,175
Cabinet	$850
Bootstrap Loader	$ 500
9 Track Magnetic Tape Unit	$11,500
Crystal Clock	$ 400

16 Channel Digital/Analog Converters	$1,000 (2 required)
Total	$39,125 [3, 13]

Compared to hardware components of another system such as an equivalent IBM 360 system to accomplish the same job, the cost to purchase the system is estimated to be $200,000. [20] Although the IBM 360 has a greater capability than the PDP8, this comparison is meaningful since large computers are used for similar applications. Use of other minicomputers could yield similar results of the PDP8.

Some hardware components differ significantly in price and would seem to be unjustified until further inspection is made. For example, in an analog system, an analog multiplier would cost approximately $15 while in a digital system a digital multiplier would cost about $125; an important advantage exists in the use of digital multipliers in that they can be time-shared among the 64 oscillators at a cost savings of 600%. Additionally, the steadily decreasing costs of large scale integration devices makes digital equipment increasingly attractive. [6]

The overall system offers enormous savings in the channel capacity needed for transmitting voice signals for a fractional increase in the cost of the terminal equipment. For assessing costs and benefits the following factors, using a single line, must be considered:

$V=CxLxF$

C cost of line per mile

L length of line in miles

V VOCOM terminal cost

F compression factor

F. HYPOTHETICAL APPLICATION

Currently, normal 3000 hertz voice grade telephone lines in the United States cost $5.48 per month per mile. [22] These lines are unconditioned , private, leased, and capable of full duplex operation. They are also capable of carrying either voice or data signals and are single channel. On short lines, of, say, less than 100 miles, the cost of terminal equipment dominates while on long lines, the lines themselves determine the costs. To illustrate an example, a single line from the Naval Postgraduate School to Washington, D.C., a distance of approximately 3000 miles, would cost $5.48 x 3000 or $16,440 per month. Multiplying this by 13, the number of autovon lines at the school, the cost goes to $213,720. It is possible, through use of the VOCOM system, to use one single existing line and through multiplexing, still have the equivalent of 13 full duplex lines. This cost savings in line usage alone would amount to $197,280. In actual practice the school only pays for the terminal equipment at the switchboard and the major expense for the autovon is borne by COMNAVTELCOM.

The autovon lines are actually switched at a switching center at Lodi California, a distance of approximately 76 air miles. The thirteen lines going to Lodi cost monthly $5,460, while if only one line were used the cost would be only $420, a significant savings. Thirteen channels could conceivably, by using the VOCOM system, reduce the line costs at a savings of $5,040 per month. One VOCOM system costs approximately $50,000 and would, through annual savings, pay for itself in less than one year.

More importantly is the fact that the secure voice feature could be added at a relatively inexpensive price. Measuring the actual value of the secure voice capability is difficult since the urgency of the needed information is subjective and requires higher level decision-making before action can be taken. The value therefore cannot be expressed in dollars but rather in time savings. In this example classified information could be exchanged between personnel from the Naval Postgraduate School and personnel from Washington D. C. in real-time as opposed to the typically delayed two or more weeks which it takes to classify, and mail the information.

A simple, single line user serves to show potential savings on line costs alone. A single line is capable of handling 4,800 bits per second. [10] By reducing the amount of data required for voice to 200 bits per second, the potential for 24 channels exists. Line conditioning, a modification to lines allowing increased data handling capability, increases further the handling capacity of this system. As an example, a 96 channel VOCOM unit could be put in to service with the new 96 channel Bell D2 channel bank enabling the equipment to operate on a single T1 line which otherwise has a capacity of only 24 channels. This immediate four-fold boost to line profitability could be further increased up to 100 times the previous traffic depending on voice fidelity and time allocation requirements.

1975 and projected 1980 costs of the VOCOM systems including hardware, software, [25] and other direct costs are illustrated below.

1975	1 system	25 systems	1000 systems
100 lines	$6,250	$2,500	$1,250
10 lines	$15,000	$6,250	$3,750
1 line	$50,000	$25,000	$25,000
1980			
100 lines	$3,750	$1,250	$750
10 lines	$10,000	$3,750	$2,500
1 line	$37,500	$15,000	$10,000

These figures are for use with trunk telephone lines. As the number of lines increases, the amount of cost decreases significanty. The system could be used as shown in figure 3. Figure 4 shows cost/benefit relationships.

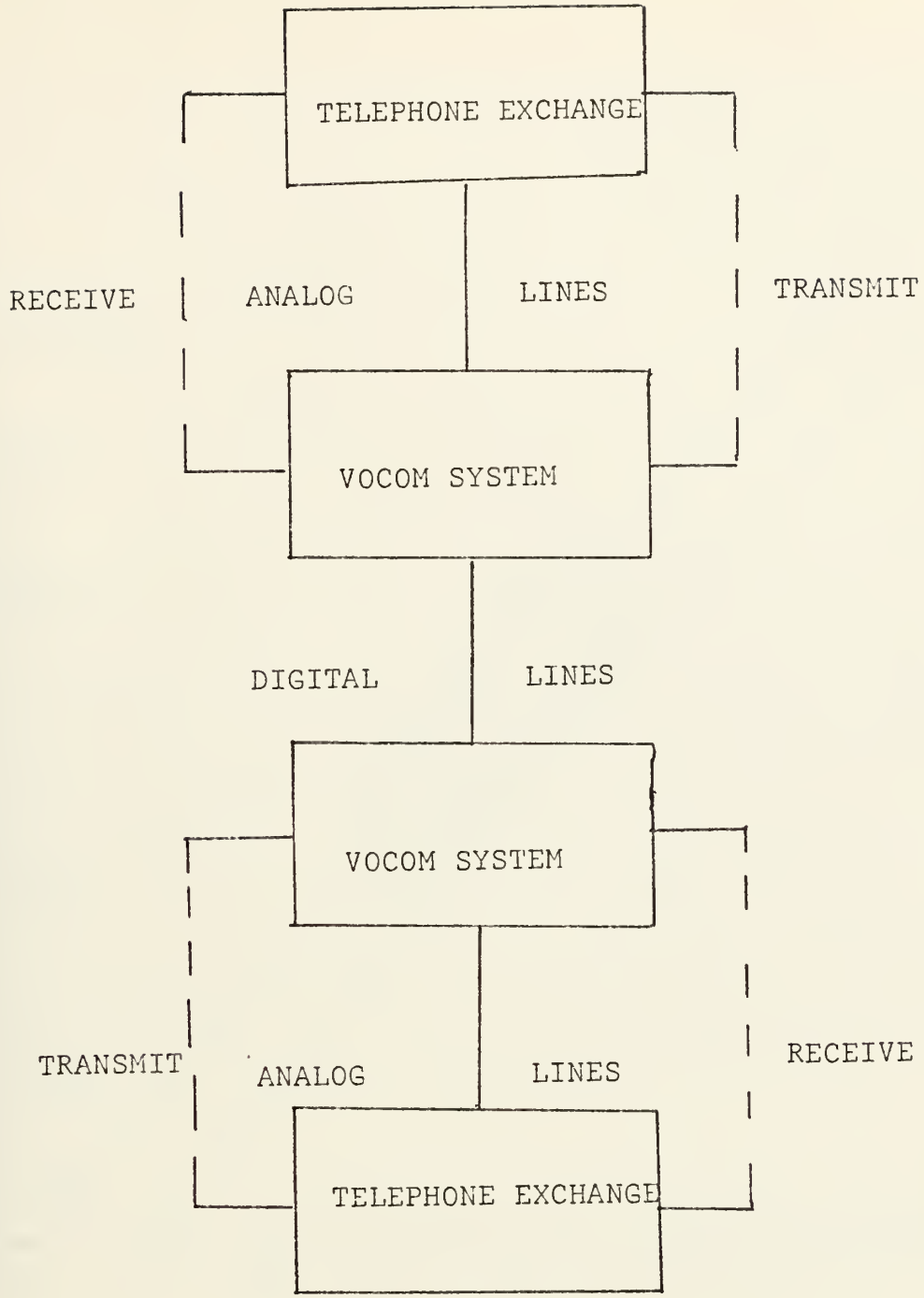


Figure 3 - TYPICAL SETUP

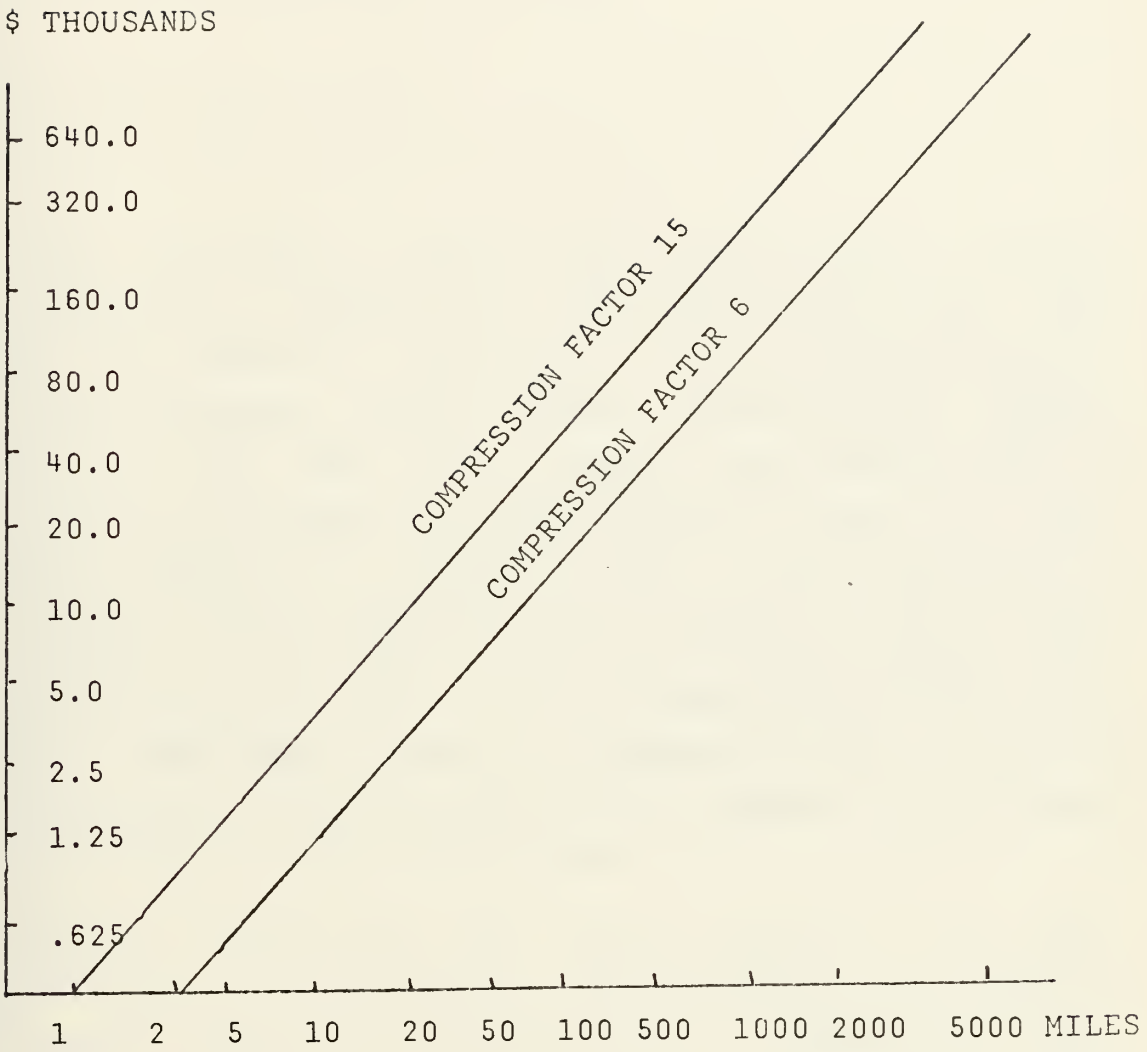


Figure 4 - COST/BENEFIT FOR CHANNEL COMPRESSION

Original development and cost of the VOCOM software is derived from the total cost of one system ($75,000) less the cost of the hardware ($40,000) or approximately $35,000. This sunk cost in technology and development will be reduced as the number of systems increases.

G. SECURING THE SYSTEM

There exist today numerous voice coding systems. Various modifications to modulation techniques incorporate some degree of bandwidth compression in the encoding process. However, no digital coding scheme satisfactorily encodes speech at less than 19.2 kilobits per second; thus, to achieve a 9.6 kilobits per second (maximum amount of data handling capacity on present lines) voice digitizer, an additional bandwidth compression of at least 2:1 must first take place. [8] These systems obviously require wider bandwidth parameters than are necessary with the VOCOM system. They also attempt to reproduce all the elements (accent, drawl, emotion) unique to the speaker but are still not successful at exact duplication.

Instead of reproducing all these elements, the VOCOM system recreates and produces a sound by using coded data of much reduced density. The sound is not a reproduced exact sound of the speaker but a synthesized recreation of it using sophisticated sound generators. For the individual user, a terminal box must be available which is simply a small portable box similar to an electronic calculator which will attach to a normal telephone handset. This terminal is forecasted to cost approximately $30 but it is expected that the user will rent the terminal along with other user services such as a supply of confidential code numbers and

directories for a particular user or group of users. By keying specified code numbers on the terminal box the user gains access to the VOCOM system and can speak through his terminal box in a secure fashion. The confidential code can ensure complete security by both changing codes at regularly scheduled intervals (hourly, daily, randomly, etc.) and can further be scrambled by changing codes automatically. In the VOCOM system any of the methods described in the introduction could be used. It has the further advantage of "multi-scrambling " from user to user. [27] It would be possible for example to have a conference call with several people talking and none of them receiving the same exact bit stream because of their own personal codes.

Software such as clumsy and bulky keylists which currently exist in the military could be reduced both in size and in complexity. Each authorized command or person could receive monthly codes instead of programming keystream generators or crypto boards. He would use his code for the particular period, punch it into the terminal, and commence communicating securely. A Naval operational commander (or anyone with proper clearance and need to know) could get real-time resolutions to problems instead of waiting for misunderstandings in messages, incomplete or delayed messages, and mistakes in messages.

IV. CONCLUSIONS

The need for secure voice communications is ever increasing both in the military and in civil circles. More importantly, the need to acquire this capability while at the same time reducing costs and improving performance is highly desirable. Present systems in use today are for the most part analog systems which require large usage of bandwidth, expensive equipment, and cumbersome, bulky, and awkward software support. Large bandwidth usage is virtually syncnymous with large costs.

In the military there is a great need for secure voice communications and prohibitive costs limit the number of available secure voice terminals. Both voice quality improvement and quantity increases are necessary in today's military forces. Most presently used systems operate in the electromagnetic spectrum above the HF range and as a consequence, much communications takes place on uncovered circuits which tends to "leak" classified information.

Present voice coding methods have room for improvement. Methods are available to both decrease costs while at the same time increasing performance. Because of the advantages, digital techniques will be employed in the future for voice communications. The system proposed here has numerous advantages because of digital techniques and the potential for changing the whole method of communicating. The most difficult problem which remains is transferring modern technology and implementing these techniques. The proposed system is readily adaptable to both presently used analog lines as well as modern,

conditioned, high data lines.

Costs of the proposed system can be reduced over a period of time and with increased numbers of the systems, costs continue to decrease. Potential savings in line usage alone have been discussed and it has been shown how the system could conceivably pay for itself over time.

The system is already in itself secure. Communications security procedures and publication handling could be designed to integrate with present procedures. An additional advantage exists in that current software requirements for coding, keylists, etc., could be reduced significantly.

Presently used voice coding systems have a synchronization process which they go through prior to establishing communications. With the proposed system, synchronous linking would be established at the patch panel either manually, or through previously programmed methods.

Bandwidth is a technical resource which must be conserved. This proposed system offers a method of conserving bandwidth by increasing the efficiency of its usage.

For military applications there exist some apparent disadvantages. Most important is in the oscillators themselves. Typically, oscillators tend to drift in frequency and tuning accuracy is difficult. Maintenance of properly tuned and stabilized oscillators may be an expensive and unforseen cost which could affect the overall system significantly.

Duplicate systems would have to be available in critical communications links. If only one system were in operation and the system became disabled because of loss of oscillator

frequency stabilization or for any other reason, a back-up system would be required thus further increasing costs.

A further disadvantage exists in that an alarm system to warn the user if he is actually talking in a secure fashion would be required. As the system exists, there is no method of determining whether the equipment is in fact operating in either a secure or an unsecure mode.

V. RECOMMENDATIONS

A continuing investigation of this proposed voice coding system is needed. Application to telephone lines have been discussed but there remains potentially dollar and bandwidth savings to be realized in HF, UHF, satellite, and even in LF and VLF applications. Use of the proposed system in these areas requires further investigation.

The proposed system should be officially investigated by the Navy in an in depth feasibility study. To ease the complications of communicating with Electronic Music Studios in London, it would be beneficial for some military unit there (not necessarily limited to the Navy) to make an on-site investigation and study. The Office of Naval Research London would be the prime candidate.

Since the system has proven itself in the civilian arena, it should be demonstrated and applied using military peripheral equipment.

The use of a programmable, changing and flexible random code changing device needs to be investigated further.

Testing of privacy and intelligibility, flexibility and security must be coordinated with the National Security Agency to find if standard requirements can be met. Reliability tests should be included.

Further design modifications should be considered for the use of microcomputers and other large scale integration devices for potential use as portable equipment in field

operations.

It is realized that Electronics Music Studios literature has provided a large portion of the data for this study and in that context it may be somewhat biased. The United States spends annually millions of dollars [2] in research and development of communications security equipment; it is hoped that some of that could be invested in this system. In any event, the initial equipment exists and secure voice communication with bandwidth reduction has been realized. It is the hope of this author that future investigation and Naval interest will lead to a complete, or at minimum a partial operational network.

LIST OF REFERENCES

1. Bac, S. A., Secure Flight Deck Communications, M.S.E.E., Thesis, U. S. Naval Postgraduate School, Monterey, 1973.

2. Boak, D., Chief of Office of Communications Security, Evaluations and Standards, presentation delivered to Information Systems Management students, U. S. Naval Postgraduate School, Monterey, January 15, 1976.

3. Broaddent, S., Customer Engineer, Digital Corporation, Santa Clara, Personal interview January 8, 1976.

4. Cary, T., "The Evolution Of Vocom From Electronic Music Techniques, unpublished paper, London, 1973.

5. Cocci, A. J., A Spread Spectrum Communication Technique, E.E. Thesis, U.S. Naval Postgraduate School, Monterey, 1973.

6. Cockerell, D., "Vocom," unpublished paper, London, 1973.

7. Eastty, P., "A New Method Of Vocom Analysis," unpublished paper, London, 1973.

8. Electromagnetics Division Institute For Basic Standards, National Bureau Of Standards Report NBSIR 73-324, Voice Privacy Equipment For Law Enforcement Communications Systems, by G. R. Sugar September, 1973.

9. Grogono, P., MUSYS, an Electronic Music Language and System, unpublished paper, London, 1973.

10. Hughes, W., Pacific Telephone, Personal Interview January 10, 15, 1976.

11. Kahn, D., The Codebreakers, Macmillan, 1967.

12. Keeton, L. L., Secure Low Cost Voice Coding Processor, M.S.E.E. Thesis, U.S. Naval Postgraduate School, Monterey, 1974.

13. Kiest, B., Digital Corporation, Personal Interview, January 7, 1976.

14. Lawson, J. "Vocom Programming 1973," unpublished paper, London, 1973.

15. Lewis P. Jr., and Heames, R. D., configuration And Management Analysis of the Naval Postgraduate School Telephone System, M.S. in Management Thesis, U.S. Naval Postgraduate School, Monterey, 1974.

16. Martin J., Systems Analysis For Data Transmission, Prentice-Hall, 1972.

17. Naval Electronics Center laboratory Report TN 2499, FLTSATCOM to AUTOSEVOCOM, System Configurations, unpublished paper prepared by L. M. Yancey and C. G. Wilhelm, 18 October, 1973.

18. Naval Electronics Laboratory Center Report TN 2180, Preliminary Specifications Secure Voice System (SVS) (WBS 131CC00), unpublished paper for NAVELEX, 13 October, 1972.

19. Naval Research Laboratory Report 2413 Survey of Speech Bandwidth Compression Techniques For H-F Secure Voice Systems, by W. M. Jewett and F. C. Kahler, March, 1972.

20. Norman, D. F., NPS Computer Center Manager, Personal Interview , January 13, 1976.

21. Oehlenschlager, J. G., A Feasibility Study of a Hybrid

Secure Voice Coding Processor, M.S.E.E., Thesis, U. S. Naval Postgraduate School, Monterey, 1972.

22. Peterson, R., Pacific Telephone, Monterey, Personal Interview, January 6, 1976.

23. Review of Department of Defense Worldwide Communications Phase II, Robert H. Mollohan, Chairman Defense Communications Subcommittee on Armed Services House of Representatives, 92nd Congress, October 12, 1972.

24. Shannon, C. E., quoted in The Codebreakers, by D. Kahn Macmillan, 1967.

25. Sutcliffe, A., "The Exploitation of Vocom," unpublished paper, London, 1973.

26. Trujillo, R., NPS Telephone Officer, Personal Interview, January 8, 1976.

27. VOCOM, Electronics Music Studios, London, 1973.

28. Zinovieff, P., "A Practical Demonstration of Vocom," unpublished paper, London, 1973.

29. Zinovieff, P., "The Future of Vocom: The System Already in Use in London," unpublished paper, London, 1973.

30. Zinovieff, P., "Vocom Transmitter-Technical Data," unpublished paper, London, 1973.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
3.	Department Chairman, Code 55 Operations Research and Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
4.	Professor Orestes M. Baycura, Code 52By Naval Postgraduate School monterey, California 93940	2
5.	Lieutenant Commander F. L. Baca USN SMC 1778 Naval Postgraduate School Monterey, California 93940	1
6.	Mr. Alan Sutcliffe Electronics Music Studios 277 Putney Bridge Road London, SW152PT England	1

Thesis 185088
B10525 Baca
c.1 A secure voice system with bandwidth reduction.